(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 120 198 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 153(4) EPC

(43) Date of publication:
18.11.2009 Bulletin 2009/47

(21) Application number: **08710899.9**

(22) Date of filing: **07.02.2008**

(51) Int Cl.:
G06Q 20/00 *(2006.01)* ***G06F 21/24*** *(2006.01)*
G06Q 10/00 *(2006.01)* ***G06Q 30/00*** *(2006.01)*
H04L 9/08 *(2006.01)*

(86) International application number:
PCT/JP2008/052009

(87) International publication number:
WO 2008/096808 (14.08.2008 Gazette 2008/33)

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR

(30) Priority: **08.02.2007 JP 2007029714**

(71) Applicant: **NTT DoCoMo, Inc.**
Chiyoda-ku
Tokyo 100-6150 (JP)

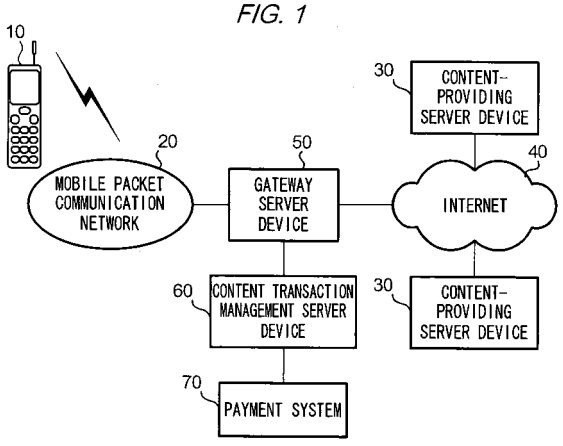
(72) Inventors:
- **ONDA, Yasushi**
  Chiyoda-ku
  Tokyo 100-6150 (JP)
- **KANO, Izua**
  Chiyoda-ku
  Tokyo 100-6150 (JP)
- **KAMIYA, Dai**
  Chiyoda-ku
  Tokyo 100-6150 (JP)
- **KUSHIDA, Yusuke**
  Chiyoda-ku
  Tokyo 100-6150 (JP)
- **MURAKAMI, Keiichi**
  Chiyoda-ku
  Tokyo 100-6150 (JP)
- **YAMADA, Eiju**
  Chiyoda-ku
  Tokyo 100-6150 (JP)
- **YAMADA, Kazuhiro**
  Chiyoda-ku
  Tokyo 100-6150 (JP)

(74) Representative: **HOFFMANN EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) CONTENT BUSINESS MANAGEMENT SERVER DEVICE, CONTENT PROVIDING SERVER DEVICE, TERMINAL, AND PROGRAM THEREOF

(57) A content transaction management server device includes: a memory storing decryption keys used in decryption of encrypted content data; a communication unit for information; a payment-request reception unit receiving, through the communication unit, a first storage address indicating a storage area where the decryption keys of encrypted content data in the memory are stored and user identifiers identifying users who are purchasers of the encrypted content data; a payment-procedure processing unit implementing payment-procedure processes related to purchase transactions of encrypted content data by a user identified by user identifiers in the payment request; and a decryption-key transmission unit that, after payment-procedure processing based on the payment-procedure processing unit is completed, reads out, from the memory, decryption keys stored in the storage area indicated by the first storage address included in the payment request and transmits, through the communication unit, the decryption keys to the transmission source of the payment request.

FIG. 1



EP 2 120 198 A1

Description

Technical field

[0001] The present invention relates to transaction of encrypted content.

Related art

[0002] Systems for delivering various content data to users of a network in exchange for payment of costs through predetermined payment processes are in widespread use. Various types of mechanisms for efficiently operating these types of systems have been proposed. For example, in the digital content transaction support system disclosed in JP-A-2004-13743, encrypted content data is stored on a server device and a decryption key for such content data is transmitted to the terminal of the purchaser after the completion of payment processes by the purchaser.

Summary

[0003] It is noted here that in cases of individual entities selling original content data, it is not easy for such entities to efficiently collect payment for such data. Namely, it is often necessary for sales to be implemented through a procedure of encrypting the original content data and registering the same on a server device on a network, requesting a deposit of payment for content data by specifying a bank account to an applicant of the content data, and transmitting decryption keys to the applicant after completing confirmation of receipt of the payment.

[0004] However, in employing this mechanism the seller of the content data is required to perform cumbersome tasks such as a confirmation of a payment received, and a further problem exists in that it may not be possible to provide immediately to an applicant content data for which the applicant has applied.

[0005] The present invention has been proposed in view of the background outlined above and aims to provide a mechanism for efficiently performing content-data transactions without requiring cumbersome tasks to be carried out by the seller or purchaser.

[0006] According to an aspect of the present invention, there is provided a content transaction management server device including: storage means for storing a decryption key used for decryption of encrypted content data; communication means for communicating information; payment-request reception means for receiving a payment request through the communication means, the payment request including a first storage address and a user identifier, the first storage address indicating a storage area in the storage means in which the decryption key is stored, the user identifier identifying a user, who is a purchaser of the encrypted content data; payment-procedure processing means for performing payment-procedure processes related to a transaction for purchase of the encrypted content data by the user identified by the user identifier included in the payment request; and decryption-key transmission means for transmitting the decryption key through the communication means to a transmission source of the payment request, after the payment-procedure processing by the payment-procedure processing means is completed, the transmitted decryption key being read out from the storage area in the storage means, the storage area being indicated by the first storage address included in the payment request.

[0007] According to an aspect of this content transaction management server device, content-data transactions can be performed efficiently without requiring cumbersome tasks to be carried out by the seller or purchaser.

[0008] This exemplary embodiment of a content transaction management server device may further include: content-data reception means for receiving, through the communication means, content data as well as a second storage address indicating a storage area of an external device; encryption means for generating encrypted content data by applying a predetermined encryption key to the received content data; storage control means for controlling the storage means to store a decryption key that is a counterpart of the encryption key used in the encryption by the encryption means; and file transmission means for transmitting a definitions file and the encrypted content data, through the communication means to a transmission source of the content data and the second storage address, the definitions file including the first storage address indicating the storage area where the decryption keys are stored and the second storage address, the encrypted content data being generated by the encryption means.

[0009] According to an aspect of this content transaction management server device, the definitions file for acquisition procedures and encrypted content data are transmitted to the source of transmission of the content data and the second storage address.

[0010] Moreover, the above exemplary embodiment may further include: content-data reception means for receiving, through the communication means, content data including a plurality of data sets, a second storage address indicating a storage area of an external device, and a data-set identifier for identifying one of the data sets included in the content data; encryption means for generating encrypted content data including an encrypted data set and unencrypted content data, by applying a predetermined encryption key to a data set specified from among the received content data by the data-set identifier; storage control means for controlling the storage means to store a decryption key that is a counterpart of the encryption key used in the encryption by the encryption means; and file transmission means for transmitting a definitions file and the encrypted content data through the communication means to a transmission source of the content data and the data-set identifiers, the definitions file including the first storage address, the

second storage address and the data-set identifier, the encrypted content data being generated by the encryption means.

[0011] According to an aspect of this content transaction management server device, the definitions file for data-set acquisition procedures and encrypted content data are transmitted to the transmission source of the content data and data-set identifiers.

[0012] In addition, the above exemplary embodiment may further include: content-data reception means for receiving, through the communication means, content data including a plurality of data sets as well as a data-set identifier for specifying a data set included in the content data; encryption means for generating encrypted content data including an encrypted data set and unencrypted content data, the encrypted data set being encrypted by applying a predetermined encryption key to a data set specified from among the received content data by the data-set identifier; storage control means for controlling the storage means to store a decryption key that is a counterpart of the encryption key used in the encryption by the encryption means; and file transmission means for transmitting, through the communication means to a transmission source of the content data and the data-set identifier, a definitions file for data-set acquisition procedures and encrypted content data, the definitions file including the first storage address and the data-set identifier, the encrypted content data being generated by the encryption means.

[0013] According to an aspect of this content transaction management server device, the definitions file for acquisition procedures and encrypted content data is transmitted to the transmission source of the content data and data-set identifiers.

[0014] According to another aspect of the invention, there is provided a content-providing server device including: storage means for storing information; communication means for communicating information; file reception means for receiving encrypted content data and a definitions file for acquisition procedures, the definitions file including a first storage address and a second storage address, the first storage address indicating a storage area in which a decryption key is stored, the decryption key being a counterpart of an encryption key used for generating the encrypted content data, the second address indicating a storage area in the storage means; storage control means for controlling the storage area to store the encrypted content data in the storage area indicated by the second storage address, and to store the definitions file in another storage area different from the storage area; file transmission means for transmitting the definitions file, the definitions file being read out from the storage means; request reception means for receiving, through the communication means, a download request including the second storage address from a transmission source of the definitions file; and encrypted-content-data transmission means for transmitting, through the communication means to a transmission source of the download request, the encrypted content data read out from the storage area in the storage means indicated by the second storage address included in the received download request.

[0015] According to an aspect of this content-providing server device, encrypted content data are transmitted to the transmission source of the download request.

[0016] According to yet another aspect of the invention, there is provided a terminal device including: storage means for storing a user identifier for identifying a user of the terminal device; communication means for communicating information; file reception means for receiving, through the communication means, a definitions file for download acquisition procedures including a first storage address and a second storage address, the first storage address indicating a storage area in a first external device in which a decryption key is stored, the decryption key being a counterpart of an encryption key used for encrypting content data, the second storage address indicating a storage area of a second external device in which the encrypted content data is stored, the encrypted content data being encrypted with the encryption key; payment-request transmission means for transmitting, through the communication means to the first external device, a payment request including the first storage address and a user identifier, is the first storage address being included in the definitions file, the user identifier being read out from the storage means; download-request transmission means for transmitting, through the communication means to the second external device, a download request including the second storage address, the second storage address being extracted from the definitions file and; content reception means for receiving, through the communication means, encrypted content data stored in a storage area of the second external device indicated by the second storage address; decryption-key reception means for receiving, through the communication means, the decryption key stored in the storage area of the first external device indicated by the first storage address; and decryption means for decrypting content data by applying the received decryption key to the received encrypted content data.

[0017] According to an aspect of this terminal device, content data is decrypted by applying received decryption keys to encrypted content data.

[0018] According to yet another aspect of the invention, there is provided A program causing a computer device to execute a process, the computer device including storage means for storing a user identifier for identifying a user of a terminal device and communication means for communicating information, the process including: receiving, through the communication means, a definitions file for download acquisition procedures including a first storage address and a second storage address, the first storage address indicating a storage area in a first external device in which a decryption key is stored, the decryption key being a counterpart of an encryption key used for encrypting content data, the second

storage address indicating a storage area of a second external device in which the encrypted content data is stored, the encrypted content data being encrypted with the encryption key; transmitting, through the communication means to the first external device, a payment request including the first storage address and a user identifier, is the first storage address being included in the definitions file, the user identifier being read out from the storage means; transmitting, through the communication means to the second external device, a download request including the second storage address, the second storage address being extracted from the definitions file and; receiving, through the communication means, encrypted content data stored in a storage area of the second external device indicated by the second storage address; receiving, through the communication means, the decryption key stored in the storage area of the first external device indicated by the first storage address; and decrypting content data by applying the received decryption key to the received encrypted content data.

[0019] According to an aspect of this program, content-data transactions can be performed efficiently without requiring cumbersome tasks to be carried out by the seller or purchaser.

Brief Description of the Drawings

[0020] Exemplary embodiments of the present invention are described in detail based on the following figures, wherein:

FIG. 1 shows an overall configuration of a content transaction system;
FIG. 2 shows a physical configuration of a mobile terminal;
FIG. 3 shows a logical configuration of a mobile terminal;
FIG. 4 shows a schematic diagram of a hardware configuration of a content transaction management server device;
FIG. 5 shows a schematic diagram of a hardware configuration of a content-providing server device;
FIG. 6 shows a flowchart showing a process for a content registration service;
FIG. 7 shows a flowchart showing a process for a content registration service;
FIG. 8 shows a marketed-content registration screen;
FIG. 9 shows a diagram showing a CPF;
FIG. 10 shows a flowchart showing a process for a content purchasing service;
FIG. 11 shows a flowchart showing a separate example of a process for a content purchasing service; and
FIG. 12 shows a flowchart showing a separate example of a process for a content purchasing service.

Description of Reference Symbols

[0021] 11: Controller. 12: Transmission and reception part. 13: Instruction input part. 14: Liquid crystal display. 15: CPU. 16: RAM. 17: ROM. 18: EEPROM. 20: Mobile packet communication network. 30: Content-providing server device. 30: Same server device. 31: Controller. 32: Communication interface. 33: Hard disk. 34: CPU. 35: RAM. 36: ROM. 40: Internet communication network. 50: Gateway server device. 60: Content transaction management server device. 60: Content transaction server device. 61: Controller. 62: Communication interface. 63: Hard disk. 64: CPU. 65: RAM. 66: ROM. 70: Payment system. 71: Browser. 72: Mailer. 73: OS. 74: Java execution environment. 77: Class library. 78: JVM. 79: JAM.

Detailed Description

[0022] An exemplary embodiment of the present invention will now be described.

[0023] First, terms used in the present exemplary embodiment will be defined. "Carrier" refers to a party that administers a mobile packet communication network. "User" refers to a party that enters into a user agreement for a mobile packet communication network with a carrier. "Content provider" refers to a party that provides services for registering content data uploaded by the user on a server device connected to the Internet and for downloading such content data in response to a purchase request from a user. "Content data" includes information expressed using at least one of text, music, and/or images, such as, for example, electronic books, music, movies, video clips, Web pages, and the like. Moreover, the concept of "content data" may also include various computer programs, such as game software, Java (registered trademark) applets, and the like, as well as function groups known as API (Application Program Interface). Furthermore, "content data" may also be various items used by a player in a role-playing game, for example. In essence, in the present exemplary embodiment, "content data" refers to electronic information provided to a user after payment procedures are completed.

[0024] The content transaction system related to the present exemplary embodiment is characterized as first transmitting a unique file known as a CPF (contents payment file) to a user applying to purchase content data registered on a server device of a content provider and, by having subsequent processes executed in accordance with descriptions in the CPF, facilitating procedures from payment to the acquisition of content data. The CPF functions as a file that defines procedures for acquiring content data, or, in other words, as a definitions file for acquisition procedures.

[0025] FIG. 1 shows an overall configuration of a content transaction system related to the present exemplary embodiment. As shown in the figure, this system includes a mobile packet communication network 20 to which a mobile terminal 10 is connected, the Internet 40 to which

a content-providing server device 30 is connected, a gateway server device 50 that intervenes between the two communication networks, a content transaction management server device 60 that functions as a proxy of the gateway server device 50, and a payment system 70. In addition, as shown in the figure, multiple content-providing server devices 30 are connected to the Internet 40. The payment system 70 is a system including various financial networks, for example, a JBA (Japanese Bankers Association) network or CAFIS (Credit and Finance Information System) network (not shown). The content transaction management server device 60 performs payment-procedure processing related to transactions of content data and requests payment processing by the payment system 70, and payment processing by the payment system 70 is thereby executed.

[0026] The mobile packet communication network 20 is an aggregation of nodes that transfer data through procedures compliant with a protocol, for example, a simplified protocol of TCP (transmission control protocol)/IP (Internet protocol) or a protocol corresponding to HTTP (hyper text transfer protocol) implemented via TCP/IP, and the like. The mobile packet communication network 20 includes a base station and a packet-subscriber processing device. The Internet 40 is an aggregation of nodes that transfer data through procedures compliant with TCP/IP or HTTP, SMTP (simple mail transfer protocol), and the like that are implemented via TCP/IP, and it includes a server device and a router.

[0027] The gateway server device 50 is a computer operating in a mobile packet gateway switching center that interconnects the mobile packet communication network 20 and the Internet 40 under the management of the carrier. Data delivered from a node of one communication network to a node of another communication network is transferred to the node of the other communication network upon having a protocol converted at the gateway server device 50.

[0028] FIG. 2 shows a physical configuration of a mobile terminal 10. The mobile terminal 10 includes a controller 11 (an example of file reception means, payment-request transmission means, download-request transmission means, content reception means, decryption-key reception means, and decryption means), a transmission and reception part 12 (an example of communication means), an instruction input part 13, and a liquid crystal display 14.

[0029] The transmission and reception part 12 performs wireless communication with a base station of the mobile packet communication network 20 under the control of the controller 11.

[0030] The instruction input part 13 includes various buttons, such as PB (push buttons) and the like, and cursor keys. When an input operation is performed by a user, the instruction input part 13 supplies to the controller 11 a signal corresponding to the input operation. The liquid crystal display 14 includes a display device such as a liquid crystal panel or the like. The liquid crystal display 14 displays a variety of information under the control of the controller 11.

[0031] The controller 11 includes a CPU 15, RAM 16, ROM 17 and EEPROM 18 (an example of memory).

[0032] The CPU 15 executes various programs stored in the ROM 17 and EEPROM 18 with using the RAM 16 as a work area.

[0033] The ROM 17 stores preinstalled programs. The preinstalled programs are programs that are stored in the ROM 17 during the process of manufacturing the mobile terminal 10. For example, the preinstalled programs can include a multitask operating system (hereinafter referred to as "multitask OS"), Java(R) platform programs, and native application programs. The multitask operating system is an operating system that supports various functions, such as allocation of virtual memory space, that is necessary for implementing virtual parallel executions of multiple tasks based on a TSS (Time-Sharing System). The Java platform programs are a program group prepared in accordance with a CDC (Connected Device Configuration) in order to implement the Java execution environment described below. The native applications are programs that implement services of the mobile terminal 10, such as telephone calls, browsing, transmission and reception of a mail, and the like. The native applications include, for example, a mailer application for receiving provided mail-transmission and -reception services and a browser application for receiving provided browsing services.

[0034] The EEPROM 18 includes a Java application storage area. Java applications are stored in this storage area. A Java application includes a Jar (Java Archive) file and an ADF (Application Descriptor File). The Jar file includes a program body, image files and sound clips used during the execution of the actual programs. The program body describes procedures of processes under Java execution environment, The ADF describes information used in the installation or startup of the program, and various attributes of the Jar file. The Java application is prepared by, for example, the carrier, and stored in, for example, the content transaction management server device 60 or a server device in the Internet 40. The Java application is downloaded from the server device in response to a request from the mobile terminal 10.

[0035] Moreover, the EEPROM 18 stores a PIN (Personal Identity Number) issued by the carrier in order to uniquely identify a user.

[0036] FIG. 3 shows a logical configuration of the mobile terminal 10, implemented by the controller 11 executing various programs stored in the ROM 16 and EEPROM 18. As shown in the figure, a browser 71, a mailer 72, and a Java execution environment 74 are implemented on an OS 73 in the mobile terminal 10 executing various programs. In the EEPROM 18, a first storage 75 and second storage 76 are reserved. The browser 71 and mailer 72 are implemented by native applications stored in the ROM 16. The browser 71 and mailer 72 provides functions of receiving and interpreting of data described

in HTML (Hyper Text Markup Language) format, and transmitting and receiving an electronic mail, and the like.

[0037] The Java execution environment 74 is implemented by the Java platform programs stored in the ROM 16. The Java execution environment 74 includes a class library 77, a JVM (Java Virtual Machine) 78, and a JAM (Java Application Manager) 79. The class library 77 includes program module groups, which are each known as a "class" and have highly versatile and specific functions, in a single file. The JVM 78 is a JVM that is optimized for the CDC, which is a configuration for a portable device loaded with a multitask OS. The JVM 78 provides functions of interpreting and executing byte codes included in a Java application. The JAM 79 provides functions of controlling downloads and installations of the Java applications.

[0038] The first storage 75 includes an storage area in which the Java applications (Jar files and ADF) downloaded under the control of the JAM 79 are stored. The second storage 76 includes a storage area for storing data generated during the execution of a Java application after the Java application is terminated. In the second storage 76, an individual storage area is allocated for an installed Java application. Data stored in a certain storage area allocated to a certain Java application is rewritable only by the Java application, and other Java applications cannot rewrite data stored in that storage area.

[0039] FIG. 4 shows a hardware configuration of the content transaction management server device 60. The server device operates under the management of a carrier. As shown in the figure, the content transaction management server device 60 includes a controller 61 (an example of payment-request reception unit, payment-procedure processing unit, decryption-key transmission unit, content-data reception unit, an encryption unit, content control unit, and file transmission unit), a communication interface 62 (an example of communication unit), and a hard disk 63 (an example of memory).

[0040] The controller 61 includes a CPU 64, a RAM 65, and a ROM 66.

[0041] The communication interface 62 controls transmission and reception of data in accordance with a protocol such as TCP/IP, HTTP, and the like.

[0042] The hard disk 63 stores a payment service control program 63a, a CPF generation service control program 63b, a decryption-key database 63c, and a content purchase application 63d.

[0043] The payment service control program 63a is a program for paying purchase costs in response to a request from the mobile terminal 10 of a user purchasing content data.

[0044] The CPF generation service control program 63b is a program for encrypting the content data and generating CPF in response to a request from the mobile terminal 10 of a user selling content data. The details of the CPF are described in the paragraph on the operational description below.

[0045] The decryption-key database 63c stores decryption keys, each of which is a counterpart of an encryption key used in the encryption of content data.

[0046] The content purchase application 63d is a unique Java application (Jar files and ADF) prepared by a carrier in order to be downloaded by the mobile terminal 10. The content purchase application 63d provides to the JVM functions such as payment of purchase cost in accordance with a CPF or decryption of content data using decryption keys.

[0047] FIG. 5 shows a hardware configuration of the content-providing server device 30. The content-providing server device 30 operates under the management of a content provider. As shown in the figure, the content-providing server device 30 includes a controller 31 (an example of file reception unit, storage control unit, request reception unit and content transmission unit), a communication interface 32 (an example of communication unit), and a hard disk 33 (an example of memory).

[0048] As in the content transaction management server device 60, the controller 31 includes a CPU 34, RAM 35, and ROM 36, and moreover, the configuration of the communication interface 32 is also identical to that of the above server device 60.

[0049] In the hard disk 33, there is reserved a storage area for storing encrypted content data, for which encryption is implemented, through the content transaction management server device 60, as well as CPF generated by the above server device 60 during the encryption.

[0050] Next, the operations of the present exemplary embodiment will be described.

[0051] The operations of the present exemplary embodiment can be classified broadly between content-registration-service processing and content-purchasing-service processing. These two processes are started by a mobile terminal 10 in which a content purchase application 63d, which is stored on the content transaction management server device 60, is downloaded. Once there is an instruction from the instruction input part 13 of the mobile terminal 10 to open the content purchase application 63d, first, a service selection screen prompting the selection of either a content registration service or a content purchasing service is displayed on a liquid crystal display 14. The content-registration-service processing or the content-purchasing-service processing is started after the respective content registration service or content purchasing service is selected through further operation of the instruction input part 13.

[0052] FIG. 6 and FIG. 7 are flowcharts showing processes for a content registration service.

[0053] A user using the content registration service operates his/her mobile terminal 10 to store in the EEPROM 18, content data created using, for example, a drawing application, composing application, or the like. The user selects the content registration service from the service selection screen upon receiving, from the content provider, an allocated URL (Uniform Resource Locator) of a storage area of the content-providing server device 30, which is reserved for the storage of the content data.

[0054] When the content registration service is selected, the controller 11 of the mobile terminal 10 transmits, to the content transaction management server device 60, a request for transmitting a marketed-content registration screen (S100). The request is transmitted through a mobile packet communication network 20 and a gateway server device to the content transaction management server device 60.

[0055] When the controller 61 of the content transaction management server device 60 receives the request, the controller 61 transmits, to the mobile terminal 10, display data of the marketed-content registration screen (S110). The display data is data describing the layout of the marketed-content registration screen using HTML (Hyper Text Markup Language).

[0056] When the controller 11 of the mobile terminal 10 receives the display data, the controller 11 controls the liquid crystal display 14 to display the marketed-content registration screen (S120).

[0057] FIG. 8 shows an example of a marketed-content registration screen. Under the character string reading "Marketed-content registration" the screen includes a first input column 91 for inputting the content name, a second input column 92 for inputting the content price, a third input column 93 for inputting attached content, and a fourth input column 94 for inputting the URL of the content, and under these, a button reading "Register" is displayed.

[0058] The user, referring to the marketed-content registration screen, inputs, into the first input column 91 and the second input column 92, respectively, the name and price of the content that the user wishes to register by operating the instruction input part 13. After that, the user operates the instruction input part 13 so as to initiate operations for attaching content data stored in the EEPROM 18. Thereby, the file name of the content data being attached is input into the third input column 93. In addition, after inputting, into the fourth input column 94, the URL of the storage area of the content-providing server device 30 in which the content data is secured for storage, the user selects the "Register" button.

[0059] When the "Register" button is selected, the controller 11 of the mobile terminal 10 transmits, to the content transaction management server device 60, a content registration request including: data indicating the content name input in the first input column 91, the price input into the second input column 92 and the URL input into the fourth input column 94; and the attached content data (S130).

[0060] When the controller 61 of the content transaction management server device 60 receives the content registration request, the controller 61 generates encrypted content data by applying a unique encryption key to the content data included in the request (S 140).

[0061] Subsequently, the controller 61 controls the decryption-key database 63c to store a decryption key that is a counterpart of the encryption key used in the encryption of Step 140 (S150).

[0062] In addition, the controller 61 generates a CPF (S160).

[0063] FIG. 9 shows an example of a CPF generated in the Step 150. As shown in the figure, the CPF includes: content-name data indicating the content name; price data indicating the price; a URL (this URL hereinafter is referred to as "first URL" and is an example of the first storage address) indicating the storage area of the decryption-key database 63c in which the decryption key of Step 150 is stored; and the URL (this URL hereinafter is referred to as "second URL" and is an example of the second storage address) input into the fourth input column 94 of the marketed-content registration screen.

[0064] The controller 61 transmits, to the mobile terminal 10, the encrypted content data generated in Step 140 and the CPF generated in Step 160 (S 170).

[0065] When the controller 11 of the mobile terminal 10 receives the encrypted content data and the CPF, the controller 11 transmits, to a content-providing server device 30, a content registration request including the encrypted content data and the CPF (S180). Here, as shown in FIG. 1, multiple content-providing server devices 30 are connected to the Internet communication network, but of these, the content registration request is transmitted with its destination being the content-providing server device 30 that has received an allocated URL (Uniform Resource Locator).

[0066] When the controller 31 of the content-providing server device 30 receives the content registration request, the controller identifies the encrypted content data and CPF from the request (S 190).

[0067] The controller 31 controls the hard disk 33 to store in the storage area indicated by the second URL included in the CPF identified in Step 190 (i.e., the storage area indicated by the URL allocated in advance for storage of the content data), the encrypted content data identified in Step 190 (S200).

[0068] Subsequently, the controller 31 controls the hard disk 33 to store in an unused storage area the CPF identified in Step 190 (S210).

[0069] The controller 31 transmits, to the mobile terminal 10, a registration completion message including a URL (this URL hereinafter is referred to as "third URL") of the storage area of the hard disk 33 in which the CPF is stored in Step 210 (S220).

[0070] When the controller 11 of the mobile terminal 10 receives the registration completion message, the controller 11 controls the EEPROM 18 to store the third URL included in the message (S230).

[0071] With the above, the content-registration-service process is completed.

[0072] FIG. 10 is a flowchart showing a process for a content purchasing service.

[0073] A user using the content-purchasing-service process selects the content purchasing service from the service selection screen upon acquiring, from a separate user who has registered encrypted content data on a content-providing server device 30 using the content reg-

istration service, the third URL indicating the storage area of a CPF of content data and storing it on the EEPROM 18 of their mobile terminal 10.

[0074] When the content purchasing service is selected, the controller 11 of the mobile terminal 10 reads out the third URL stored in the EEPROM 18 and transmits, to the content-providing server device 30, a CPF transmission request including the third URL (S300).

[0075] When the controller 31 of the content-providing server device 30 receives the CPF transmission request, the controller 31 transmits, to the mobile terminal 10, the CPF stored in the hard disk 33 indicated by the third URL included in the request (S310).

[0076] When the controller 11 of the mobile terminal 10 receives the CPF, the controller 11 extracts, from the CPF, the content-name data, price data, first URL, and second URL (S320).

[0077] The controller 11 controls the liquid crystal display 14 to display a content purchase confirmation screen obtained by embedding, in a predetermined form, the content-name data and price data extracted in Step 320 (S330).

[0078] Displayed on the content purchase confirmation screen are the content name, which is indicated by the content name data, and the price, which is indicated by the price data, and under these are displayed a character string reading "Would you like to purchase this content?" and a button reading "Purchase."

[0079] The user referring to the content purchase confirmation screen selects the "Purchase" button through operations of the instruction input part 13.

[0080] If the "Purchase" button is selected, the controller 11 of the mobile terminal 10 transmits, to the content transaction management server device 60, a payment request including the content-name data, price data, and first URL extracted in Step 320 and the PIN code read out from the EEPROM 18 (S340).

[0081] If the content transaction management server device 60 receives the payment request, the controller 61 performs payment processing of the cost of the content data (S350). Specifically, the controller identifies, from a packet-communication-charge management database in a mobile packet gateway switching center, a call charge record of a user corresponding to the PIN code included in the payment request and adds the price data included in the payment request to the sum total of the call charge stored in the identified record. Thereby, the purchase amount of the content data is recorded in the calling rate claimed by the carrier from the user who is the purchaser. In this way, the process for determining the money amount claimed by a user is a payment-procedure process using the content transaction management server device 60.

[0082] Moreover, if the money amount determined through this type of payment-procedure process is reported to a payment system 70 and payment processing is requested, the payment system 70 withdraws the money amount from the bank account of the user who is the purchaser. At this time, the bank account used is a bank account that is pre-registered when the user enters into the user agreement with the carrier.

[0083] At the same time, regarding the user who is the seller, the controller 61 performs processing to provide the money amount equivalent to the price data included in the payment request. Specifically, the controller 61 identifies, from the packet-communication-charge management database, a call charge record of the user who is the seller and subtracts the price data included in the payment request from the sum total of the call charge stored in the identified record. Thereby, the calling rate claimed by the user who is the seller enters a state in which the sales total of the content data is deducted. Moreover, the calling rate from which the sales total is deducted is paid by the above payment system. In addition, if the sum total of the call charge becomes negative upon subtracting the price data, the negative amount is registered in the packet-communication-charge management database. In this case, the payment system 70 may perform processing to deposit the negative money amount into the bank account of the user who is the seller by using the money amount collected from the purchaser as funds.

[0084] If the controller 61 completes the payment processing, the controller 61 reads out the decryption key stored in the storage area of the decryption-key database 63c indicated by the first URL included in the payment request and transmits, to the mobile terminal 10, a payment completion message including the decryption key (S360).

[0085] If the mobile terminal 10 receives the payment completion message, the controller 11 controls the EEPROM 18 to store the decryption key included in the message (S370).

[0086] Subsequently, the controller 11 transmits, to the content-providing server device 30, a download request including the second URL extracted in Step 320 (S380).

[0087] If the content-providing server device 30 receives the download request, the controller 31 transmits, to the mobile terminal 10, the encrypted content data stored in the storage area of the hard disk 33 indicated by the second URL included in the request (S390).

[0088] If the mobile terminal 10 receives the encrypted content data, the controller 11 restores the content data by applying the decryption key to the encrypted content data (S400), the decryption key being stored in the EEPROM 18 in Step 370 and being read out from the EEPROM 18. The restored content data is played in response to, as a trigger, a predetermined operation through the instruction input part 13.

[0089] With the above, the content-purchasing-service process is completed.

[0090] In the present exemplary embodiment described above, when a user transmits original content data from the mobile terminal 10 to the content transaction management server device 60, the content transaction management server device 60 encrypts the content

data. The content transaction management server device 60 returns the encrypted content data and CPF obtained through encryption to the mobile terminal 10. The content data and CPF are registered on the content-providing server device 30. The CPF includes a first URL, which is a URL of a storage area of the content transaction server device 60 in which a decryption key that is a counterpart of the encryption key used in the encryption is stored, and a second URL, which is a URL of a storage area of the content-providing server device 30 in which the encrypted content data is stored. When the mobile terminal 10 of the user purchasing the content sequentially transmits requests for the first URL and second URL included in the CPF, processes from the payment of compensation for the content to acquisition of the content are performed automatically.

[0091] In this way, by variously coordinating the mobile terminal 10, the content transaction management server device 60, and the content-providing server device 30 and executing a sequence of operations related to content-data transactions, it is possible to efficiently perform content-data transactions without requiring the conventional cumbersome tasks by either the seller or purchaser.

[0092] Moreover, the following is a further detailed description of the respective merits for the seller and the purchaser.

[0093] First, the seller can easily obtain a CPF and encrypted content data by registering content data on the content transaction management server device 60. Furthermore, the seller may sell content simply through operations of coordinating the obtained CPF and encrypted content data and storing the CPF and encrypted content in a downloadable state on the content-providing server device 30. Consequently, the merits for the seller are that there is no need to prepare encryption software and no need to establish a payment system.

[0094] The purchaser may obtain the CPF by accessing the content-providing server device 30 and specifying the desired content data, and may purchase the content data simply through relatively simple operations using the CPF.

[0095] First, when the purchaser refers to the CPF obtained using their personal mobile terminal 10 and performs operations for purchasing the content data, the mobile terminal 10 transmits, to the content transaction management server device 60, a payment request including the first URL, which refers to the storage area of the decryption key, the PIN code, and the like. In response to this request, the content transaction management server device 60 performs payment procedures for the user corresponding to the PIN code and also reads out the decryption key from the storage area indicated by the first URL and transmits the decryption key to the mobile terminal 10. At this stage, the purchaser may complete the payment procedure, which is absolutely imperative for the content-data transaction, and may also obtain the decryption key necessary for the decryption of the encrypted content data. If the decryption key may be obtained at approximately the same time that the payment procedure is completed as described above, all that subsequently remains is a simple operation for obtaining the encrypted content data.

[0096] Subsequently, the purchaser performs operations for requesting encrypted content data using the mobile terminal 10. In response to the operations, the mobile terminal 10 transmits, to the content-providing server device 30, a download request including the second URL. In response to this request, the content-providing server device 30 reads out the encrypted content data from the storage area indicated by the second URL and transmits it to the mobile terminal 10. The mobile terminal 10 decrypts the encrypted content data using the previously obtained decryption key and obtains the content data. In this way, the operations for acquiring the content data are not very different from standard procedures for downloading content data on the Web, for example, and the operational burden imposed on the purchaser is very low.

Further Embodiments

[0097] Various modified exemplary embodiments are possible for the present invention. The modified examples described below may also be used in combinations of two or more.

[0098] A configuration in which the content purchase application, instead of being a Java application operating in a Java execution environment, is preliminarily stored in the ROM 16 of a mobile terminal 10 as a native application may also be used.

[0099] In the above exemplary embodiment, the content purchase application is implemented in the mobile terminal 10 (i.e., a cellular phone handset that may access an Internet 40 intermediated by a mobile packet communication network 20), but similar functions may be obtained even if an application of the same type were implemented on a personal computer that may directly access the Internet 40.

[0100] Moreover, in the above exemplary embodiment, it is presumed that the person (the seller) registering the content data subject to sales on the content-providing server device 30 is a party who has entered into a user agreement for a mobile packet communication network with the carrier (i.e., a user). However, the seller is not limited to a party who has entered into a user agreement for a mobile packet communication network with the carrier, and may simply be a party having a communication terminal that may establish a communication connection with the content transaction management server device 60 and/or content-providing server device 30.

[0101] Regarding the method for determining the price of the content, a wide range of variations may be conceived. In the exemplary embodiment, the price is determined on the basis of each individual content, but the price may also be determined on the basis of the period

of use of the content data. Specifically, the user who is the seller, when registering the content price on the marketed-content registration screen, registers a period and a compensation (price) for the act of using the content within that period and submits these to the purchaser. For example, if the seller wishes to provide, to the purchaser, a certain content for 100 yen per month, they register "1 month" as the "period" and "100 yen" as the "price," and this information is described in the CPF. In this case, the controller 11 of the mobile terminal 10 of the purchaser limits the period of use of the content in accordance with the details described in the CPF. That is, the controller 11 permits use of the content (e.g., start-up, execution, playing, transfer, and the like of the content data) during the period described in the CPF, but once the period described in the CPF has elapsed, the controller 11 does not permit use of the content.

[0102] Moreover, there is also a wide range of variations for the payment procedure.

[0103] In the exemplary embodiment, the bank account used for payment is a bank account that is registered in advance when the user enters into the user agreement with the carrier. However, as alternatives, for example, a bank account used for payments for a credit card owned by the user may be used, or a bank account used through a credit function implemented on the mobile terminal 10 may be used.

[0104] Furthermore, payments may be made using an electronic value implemented on the mobile terminal 10. In this case, the payment-procedure process of the content transaction management server device 60 is as follows.

[0105] If the content transaction management server device 60 receives the payment request, the controller 61 requests, from the mobile terminal 10 corresponding to the PIN code included in the payment request, the electronic value equivalent to the price data included in the payment request. In response to this request, the mobile terminal 10 subtracts, from the electronic value stored therein, the requested electronic value. If the mobile terminal 10 completes the subtraction process, the mobile terminal 10 reports this to the content transaction management server device 60.

[0106] In addition, the payment is not limited to using currency and may use points that may be converted into some privilege for the user.

[0107] Moreover, only a part of the data sets included in the content data may be encrypted. For example, if the content data is software providing a role-playing game, data showing an item, for example a weapon or the like used by characters in the game, is an example of the above part of data sets. In this case, in addition to the first URL and second URL described in the exemplary embodiment, multiple data-set identifiers attached to each item are described in the CPF. The first URL indicates the storage area in which the decryption keys for decrypting each of the data sets attached with the data-set identifiers.

[0108] The following is an explanation of the details centering on points of difference from the above exemplary embodiment.

[0109] In FIG. 6, when the content registration service is selected, the controller 11 of the mobile terminal 10 transmits, to the content transaction management server device 60, a request for a transmission of the marketed-content registration screen (S 100). If the content transaction management server device 60 receives the request, the controller 61 transmits, to the mobile terminal 10, display data of the marketed-content registration screen (S110). If the mobile terminal 10 receives the display data, the controller 11 displays the marketed-content registration screen on the liquid crystal display 14 (S 120). In addition to the first input column 91 for inputting the content name, the second input column 92 for inputting the price of the content, the third input column 93 for inputting the attached content, and the fourth input column 94 for inputting the content URL, which are shown in FIG. 8, the marketed-content registration screen is set with a fifth input column for inputting data-set identifiers allocated to the data sets (items used by characters in this example).

[0110] The user, referring to the marketed-content registration screen, after inputting the content name and price of the content they are registering into the first input column 91 and the second input column 92, performs operations for attaching the content data stored in the EEPROM 18 through operations of the instruction input part 13. Thereby, the file name of the content data to be attached is input into the third input column 93. Additionally, after inputting, into the fourth input column 94, the URL of the storage area of the content-providing server device 30 secured for storage of the content data and inputting, into the fifth input column, the data-set identifiers allocated to the data sets, the user selects the "Register" button. In addition, multiple data-set identifiers may be input. When the "Register" button is selected, the controller 11 of the mobile terminal 10 transmits, to the content transaction management server device 60, a content registration request including: data indicating the content name input into the first input column 91, the price input into the second input column 92, and the URL input into the fourth input column 94; the data-set identifiers input into the fifth input column; and the attached content data (S130). If the content transaction management server device 60 receives the content registration request, the controller 61 generates encrypted content data by applying unique encryption keys for only the data sets for which the data-set identifiers are allocated from among the content data included in the request (S 140). Therefore, the encrypted content data includes encrypted data sets and non-encrypted data sets. At this time, if there are multiple data-set identifiers, encryption is conducted by applying different encryption keys for each data set for which a data-set identifier is allocated. Finally, the controller 61 stores, in the decryption-key database 63c, the decryption keys that is a counterpart of the encryption keys used

in the encryption of Step 140 (S 150).

[0111] In addition, the controller 61 generates the CPF (S160). In addition to the content-name data indicating the content name, the price data indicating the price, and the first URL and the second URL, the CPF includes the above data-set identifiers. The controller 61 transmits, to the mobile terminal 10, the encrypted content data generated in Step 140 and the CPF generated in Step 160 (S170). If the mobile terminal 10 receives the encrypted content data and CPF, the controller 11 transmits, to the content-providing server device 30, a content registration request including the encrypted content data and CPF (S 180). If the content-providing server device 30 receives the content registration request, the controller 31 identifies the encrypted content data and CPF from the request (S190). Next, in FIG. 7, the controller 31 stores the encrypted content data identified in Step 190 in the storage area of the hard disk 33 indicated by the second URL included in the CPF identified in Step 190 (i.e., the storage area indicated by the URL allocated in advance for storage of the content data) (S200).

[0112] Subsequently, the controller 31 stores the CPF identified in Step 190 in an unused storage area of the hard disk 33 (S210). The controller 31 transmits, to the mobile terminal 10, a registration completion message including the URL (this URL shall hereinafter be referred to as "third URL") of the storage area of the hard disk 33 in which the CPF is stored in Step 210 (S220). If the mobile terminal 10 receives the registration completion message, the controller 11 controls the EEPROM 18 to store the third URL included in the message (S230).

[0113] Next, the content-purchase-service process is described with reference to FIG. 11. In FIG. 11, the same reference numerals are used for processes that are nearly identical to those in FIG. 10.

[0114] The user using the content purchase service selects the content purchase service from the service selection screen upon acquiring the third URL indicating the storage area of the CPF of the content data from a separate user who has registered encrypted content data onto the content-providing server device 30 using the content registration service, and storing the third URL in the EEPROM 18 of their personal mobile terminal 10. When the content purchase service is selected, the controller 11 of the mobile terminal 10 reads out the third URL from the EEPROM 18 and transmits, to the content-providing server device 30, a CPF transmission request including the third URL (S300). If the content-providing server device 30 receives the CPF transmission request, the controller 31 transmits, to the mobile terminal 10, the CPF stored on the hard disk 33 indicated by the third URL included in the request (S310).

[0115] If the mobile terminal 10 receives the CPF, the controller 11 extracts the content-name data, the price data, the first URL, and the second URL from the CPF (S320). The controller 11 displays, on the liquid crystal display 14, a content purchase confirmation screen obtained by embedding, in a predetermined form, the content-name data and price data extracted in Step 320 (S330). Then, when the "Purchase" button is selected, the controller of the mobile terminal 10 transmits, to the content transaction management server device 60, a payment request including the content-name data and price data extracted in Step 320 and a PIN code read out from the EEPROM 18 (S340). If the content transaction management server device 60 receives the payment request, the controller 61 performs payment processing of the cost of the content data (S350) and transmits, to the mobile terminal 10, a payment completion message (S360). If the mobile terminal 10 receives the payment completion message, the controller 11 transmits, to the content-providing server device 30, a download request including the second URL extracted in Step 320 (S380).

[0116] If the content-providing server device 30 receives the download request, the controller 31 transmits, to the mobile terminal 10, the encrypted content data stored in the storage area of the hard disk 33 indicated by the second URL included in the request (S390). If the mobile terminal 10 receives the encrypted content data , the controller 11 plays, opens, and executes the encrypted content data (S410). At this time, because only a part of the data sets of the encrypted content data are encrypted, the controller 11 may, with the exception of parts that are encrypted within the encrypted content data, play, open, and execute. The user, in the course of implementing the content data, which is a role-playing game in this example, will use items prepared in advance in accordance with progress in the game. In this case, when there is an instruction for an item that the user wishes to use, the controller 11 transmits, to the content transaction management server device 60, a request including the first URL and PIN code corresponding to the data-set identifier for the item (S420). The controller 61 of the content transaction management server device 60 performs payment processing of the cost of the item specified by the data-set identifier (S430). Specifically, the controller 61 identifies, from the packet-communication-charge management database, the call charge record of the user corresponding to the PIN code included in the payment request and adds, to the sum total of the call charge stored in the identified record, the predetermined price data corresponding to the item. Thereby, the purchase amount of the item is recorded in the calling rate claimed by the carrier from the user who is the purchaser. Then, when the money amount determined upon completion of this type of payment-procedure processing is reported to the payment system 70 and payment processing is requested, the payment system 70 withdraws the money amount from the bank account of the user who is the purchaser. At the same time, regarding the user who is the seller, the controller 61 performs processing to provide the money amount equivalent to the price data included in the payment request.

[0117] If the controller 61 has completed the payment processing, the controller 11 reads out the decryption key stored in the storage area of the decryption-key da-

tabase 63c indicated by the first URL included in the above request and transmits, to the mobile terminal 10, a payment completion message including the decryption key (S440). If the mobile terminal 10 receives the payment completion message, the controller 11 controls the EEPROM 18 to store the decryption key included in the message (S450). Subsequently, the controller 11 restores the item by applying the decryption key to the above data set (S460), the decryption key being read out from the EEPROM 18. The restored item is used by the character in the role-playing game.

[0118] In addition, in the above example, the first URL and the data-set identifiers are described in the CPF, and the second URL may not be described. In this case, the encrypted content data is not provided to the mobile terminal 10 through the content-providing server device 30 and may be provided to the mobile terminal 10 through a separate arbitrary method. Finally, after the encrypted content data is stored by the mobile terminal, the processes from S410 onward in FIG. 11 that are described above are performed.

[0119] The hardware configurations of the mobile terminal, content transaction management server device, and content-providing server device are not limited to each of those shown in FIG. 2, FIG. 4, and FIG. 5. If the required configuration may be implemented, these devices may have any type of hardware configuration. For example, in the exemplary embodiment described above, the controller 61 of the content transaction management server device 60 includes multiple functions, specifically, the functions of the payment-request reception means, the payment-procedure processing means, the decryption-key transmission means, the content-data reception means, the encryption means, the storage control means, and the file transmission means. However, at least one of these functions may be implemented using a hardware component separate from the controller 61.

[0120] The programs that are executed by controller 11, controller 31, or controller 61 in the exemplary embodiment described above may be provided in a state of storage on a computer-readable storage medium, such as a magnetic recording medium (magnetic tape, magnetic disk (HDD (Hard Disk Drive), FD (Floppy Disk)), or the like), an optical recording medium (optical disk (CD (Compact Disc), DVD (Digital Versatile Disc)), or the like), a magneto-optical medium, a semiconductor memory (flash ROM or the like), or the like. Moreover, the programs may also be downloaded through a network such as the Internet.

Claims

1. A content transaction management server device comprising:

   storage means for storing a decryption key used for decryption of encrypted content data;

   communication means for communicating information;

   payment-request reception means for receiving a payment request through the communication means, the payment request including a first storage address and a user identifier, the first storage address indicating a storage area in the storage means in which the decryption key is stored, the user identifier identifying a user, who is a purchaser of the encrypted content data;

   payment-procedure processing means for performing payment-procedure processes related to a transaction for purchase of the encrypted content data by the user identified by the user identifier included in the payment request; and

   decryption-key transmission means for transmitting the decryption key through the communication means to a transmission source of the payment request, after the payment-procedure processing by the payment-procedure processing means is completed, the transmitted decryption key being read out from the storage area in the storage means, the storage area being indicated by the first storage address included in the payment request.

2. The content transaction management server device according to Claim 1, further comprising:

   content-data reception means for receiving, through the communication means, content data as well as a second storage address indicating a storage area of an external device;

   encryption means for generating encrypted content data by applying a predetermined encryption key to the received content data;

   storage control means for controlling the storage means to store a decryption key that is a counterpart of the encryption key used in the encryption by the encryption means; and

   file transmission means for transmitting a definitions file and the encrypted content data, through the communication means to a transmission source of the content data and the second storage address, the definitions file including the first storage address indicating the storage area where the decryption keys are stored and the second storage address, the encrypted content data being generated by the encryption means.

3. The content transaction management server device according to Claim 1, further comprising:

   content-data reception means for receiving, through the communication means, content data including a plurality of data sets, a second storage address indicating a storage area of an

external device, and a data-set identifier for identifying one of the data sets included in the content data;

encryption means for generating encrypted content data including an encrypted data set and unencrypted content data, by applying a predetermined encryption key to a data set specified from among the received content data by the data-set identifier;

storage control means for controlling the storage means to store a decryption key that is a counterpart of the encryption key used in the encryption by the encryption means; and

file transmission means for transmitting a definitions file and the encrypted content data through the communication means to a transmission source of the content data and the data-set identifiers, the definitions file including the first storage address, the second storage address and the data-set identifier, the encrypted content data being generated by the encryption means.

4. The content transaction management server device according to Claim 1, further comprising:

content-data reception means for receiving, through the communication means, content data including a plurality of data sets as well as a data-set identifier for specifying a data set included in the content data;

encryption means for generating encrypted content data including an encrypted data set and unencrypted content data, the encrypted data set being encrypted by applying a predetermined encryption key to a data set specified from among the received content data by the data-set identifier;

storage control means for controlling the storage means to store a decryption key that is a counterpart of the encryption key used in the encryption by the encryption means; and

file transmission means for transmitting, through the communication means to a transmission source of the content data and the data-set identifier, a definitions file for data-set acquisition procedures and encrypted content data, the definitions file including the first storage address and the data-set identifier, the encrypted content data being generated by the encryption means.

5. A content-providing server device comprising:

storage means for storing information;

communication means for communicating information;

file reception means for receiving encrypted content data and a definitions file for acquisition procedures, the definitions file including a first storage address and a second storage address, the first storage address indicating a storage area in which a decryption key is stored, the decryption key being a counterpart of an encryption key used for generating the encrypted content data, the second storage address indicating a storage area in the storage means;

storage control means for controlling the storage area to store the encrypted content data in the storage area indicated by the second storage address, and to store the definitions file in another storage area different from the storage area;

file transmission means for transmitting the definitions file, the definitions file being read out from the storage means;

request reception means for receiving, through the communication means, a download request including the second storage address from a transmission source of the definitions file; and

encrypted-content-data transmission means for transmitting, through the communication means to a transmission source of the download request, the encrypted content data read out from the storage area in the storage means indicated by the second storage address included in the received download request.

6. A terminal device comprising:

storage means for storing a user identifier for identifying a user of the terminal device;

communication means for communicating information;

file reception means for receiving, through the communication means, a definitions file for download acquisition procedures including a first storage address and a second storage address, the first storage address indicating a storage area in a first external device in which a decryption key is stored, the decryption key being a counterpart of an encryption key used for encrypting content data, the second storage address indicating a storage area of a second external device in which the encrypted content data is stored, the encrypted content data being encrypted with the encryption key;

payment-request transmission means for transmitting, through the communication means to the first external device, a payment request including the first storage address and a user identifier, is the first storage address being included in the definitions file, the user identifier being read out from the storage means;

download-request transmission means for transmitting, through the communication means to the second external device, a download re-

quest including the second storage address, the second storage address being extracted from the definitions file and;

content reception means for receiving, through the communication means, encrypted content data stored in a storage area of the second external device indicated by the second storage address;

decryption-key reception means for receiving, through the communication means, the decryption key stored in the storage area of the first external device indicated by the first storage address; and

decryption means for decrypting content data by applying the received decryption key to the received encrypted content data.

7. A program causing a computer device to execute a process, the computer device including storage means for storing a user identifier for identifying a user of a terminal device and communication means for communicating information, the process comprising:

receiving, through the communication means, a definitions file for download acquisition procedures including a first storage address and a second storage address, the first storage address indicating a storage area in a first external device in which a decryption key is stored, the decryption key being a counterpart of an encryption key used for encrypting content data, the second storage address indicating a storage area of a second external device in which the encrypted content data is stored, the encrypted content data being encrypted with the encryption key;

transmitting, through the communication means to the first external device, a payment request including the first storage address and a user identifier, is the first storage address being included in the definitions file, the user identifier being read out from the storage means;

transmitting, through the communication means to the second external device, a download request including the second storage address, the second storage address being extracted from the definitions file and;

receiving, through the communication means, encrypted content data stored in a storage area of the second external device indicated by the second storage address;

receiving, through the communication means, the decryption key stored in the storage area of the first external device indicated by the first storage address; and

decrypting content data by applying the received decryption key to the received encrypted content data.

FIG. 1

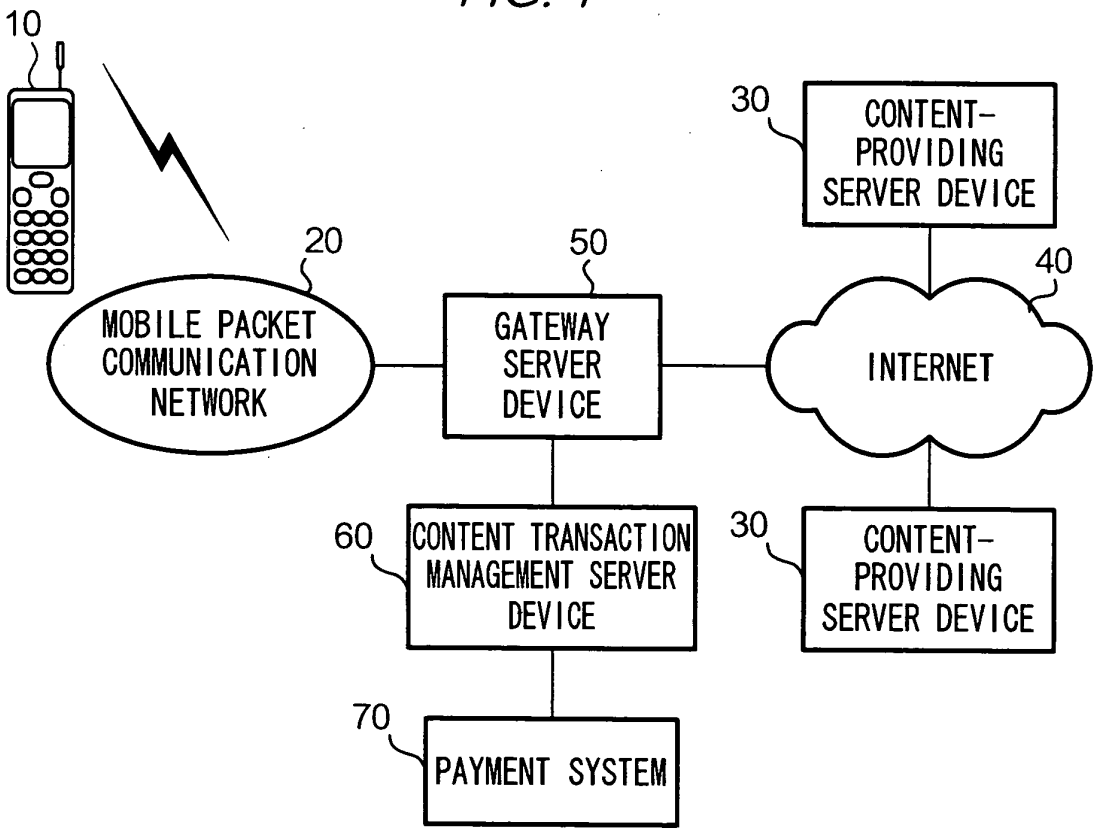

10
30
CONTENT-PROVIDING SERVER DEVICE
20
50
40
MOBILE PACKET COMMUNICATION NETWORK
GATEWAY SERVER DEVICE
INTERNET
60
CONTENT TRANSACTION MANAGEMENT SERVER DEVICE
30
CONTENT-PROVIDING SERVER DEVICE
70
PAYMENT SYSTEM

FIG. 2

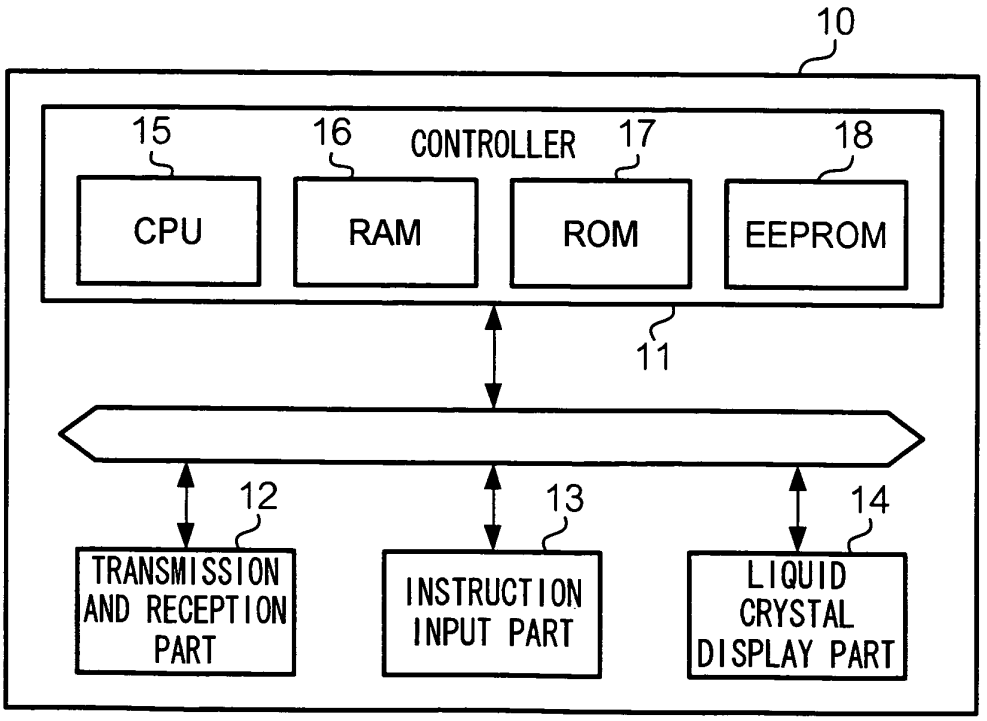

10
15
16
CONTROLLER
17
18
CPU
RAM
ROM
EEPROM
11
12
13
14
TRANSMISSION AND RECEPTION PART
INSTRUCTION INPUT PART
LIQUID CRYSTAL DISPLAY PART

FIG. 3

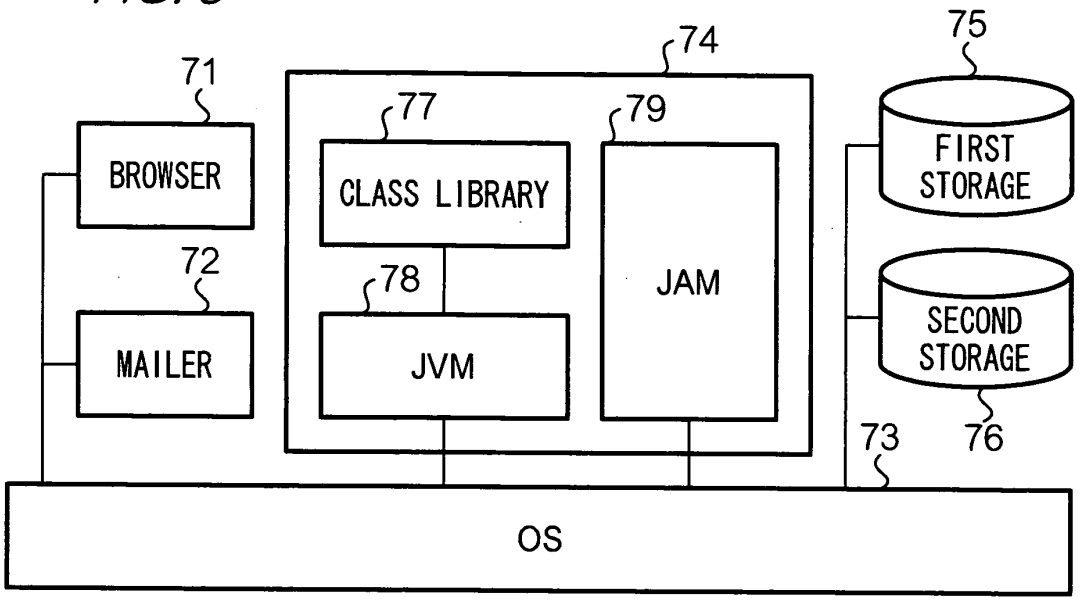

71
BROWSER
72
MAILER
74
77
CLASS LIBRARY
78
JVM
79
JAM
75
FIRST STORAGE
SECOND STORAGE
76
73
OS

FIG. 4

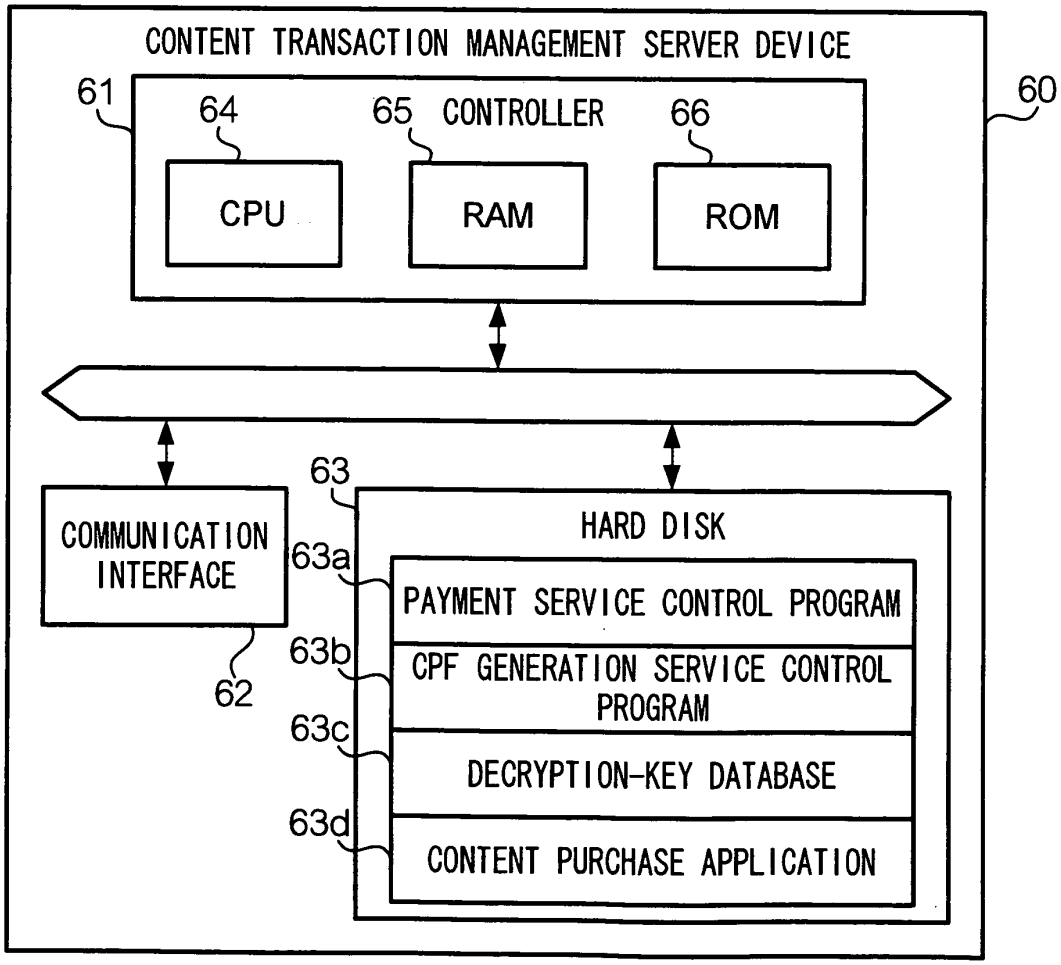

CONTENT TRANSACTION MANAGEMENT SERVER DEVICE
60
61
64
CPU
65
CONTROLLER
RAM
66
ROM
COMMUNICATION INTERFACE
62
63
HARD DISK
63a
PAYMENT SERVICE CONTROL PROGRAM
63b
CPF GENERATION SERVICE CONTROL PROGRAM
63c
DECRYPTION-KEY DATABASE
63d
CONTENT PURCHASE APPLICATION

FIG. 5

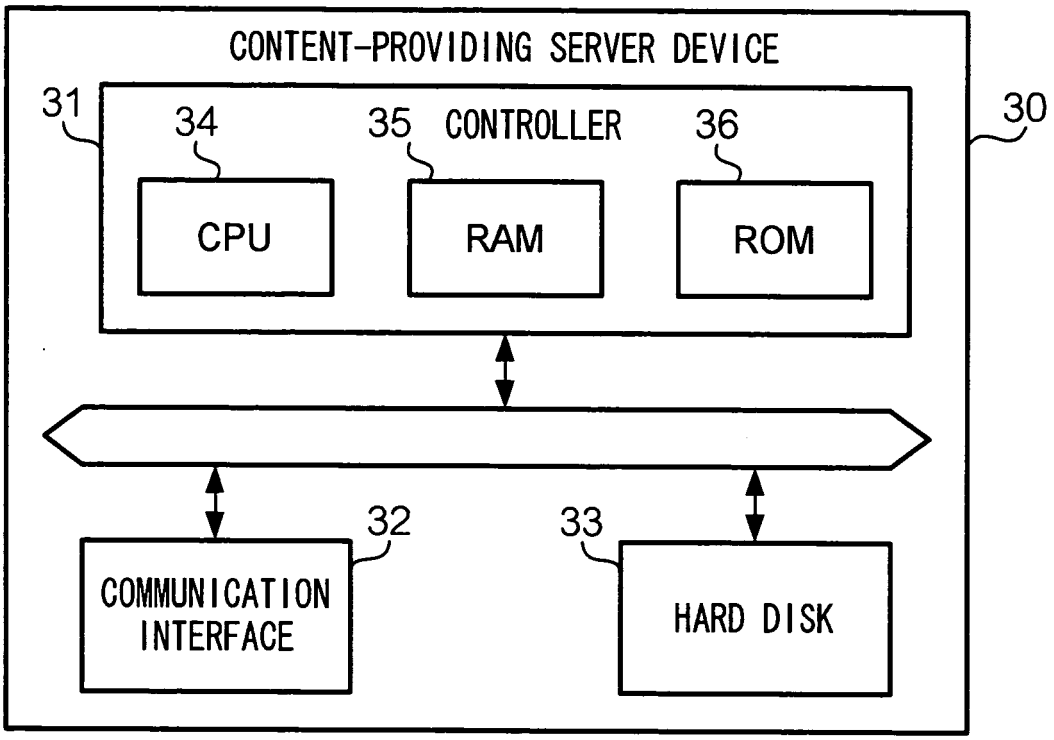

CONTENT-PROVIDING SERVER DEVICE
31
34
35
CONTROLLER
36
30
CPU
RAM
ROM
32
33
COMMUNICATION INTERFACE
HARD DISK

FIG. 6

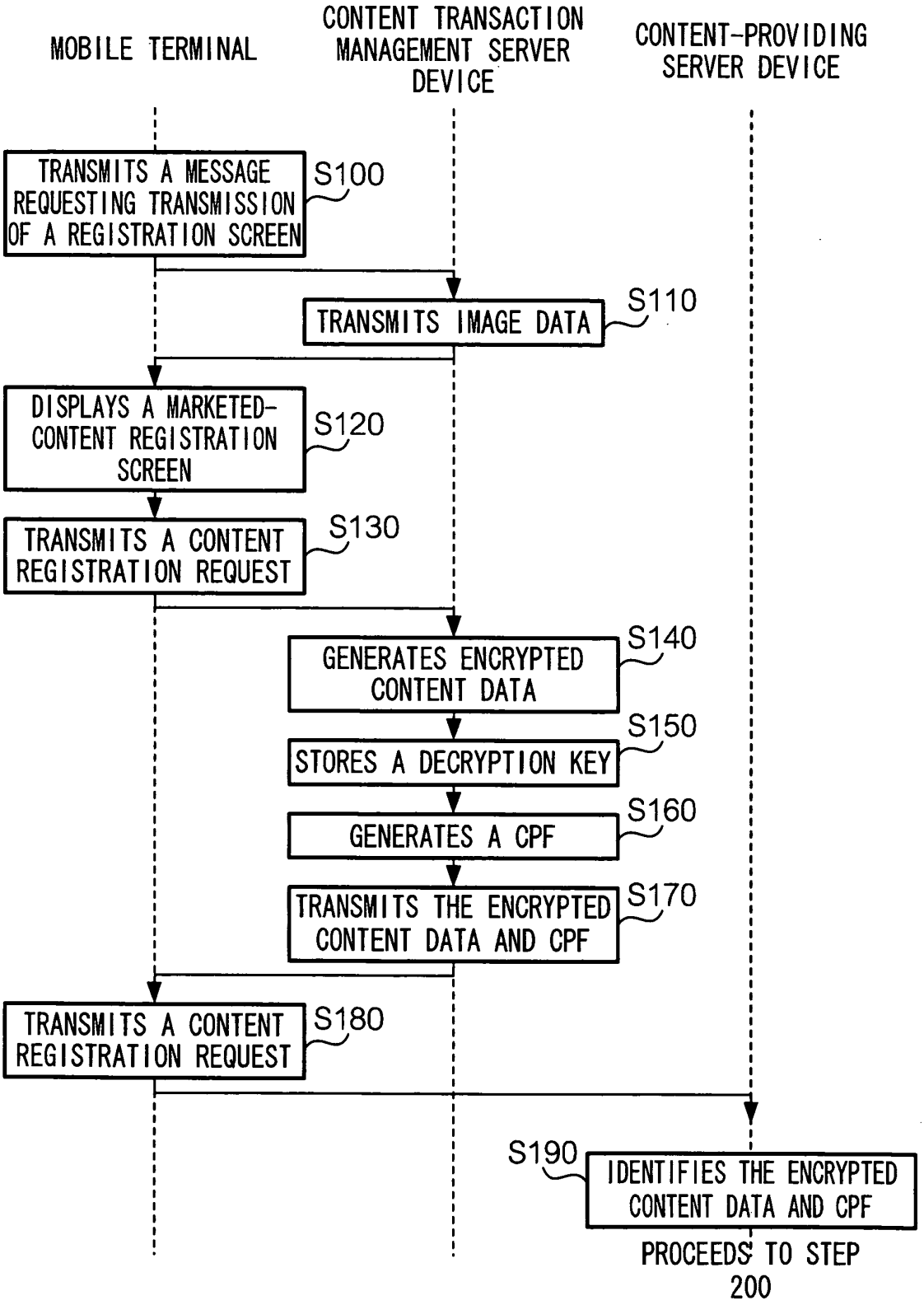

MOBILE TERMINAL
CONTENT TRANSACTION MANAGEMENT SERVER DEVICE
CONTENT-PROVIDING SERVER DEVICE
TRANSMITS A MESSAGE REQUESTING TRANSMISSION OF A REGISTRATION SCREEN
S100
TRANSMITS IMAGE DATA
S110
DISPLAYS A MARKETED-CONTENT REGISTRATION SCREEN
S120
TRANSMITS A CONTENT REGISTRATION REQUEST
S130
GENERATES ENCRYPTED CONTENT DATA
S140
STORES A DECRYPTION KEY
S150
GENERATES A CPF
S160
TRANSMITS THE ENCRYPTED CONTENT DATA AND CPF
S170
TRANSMITS A CONTENT REGISTRATION REQUEST
S180
S190
IDENTIFIES THE ENCRYPTED CONTENT DATA AND CPF
PROCEEDS TO STEP 200

FIG. 7

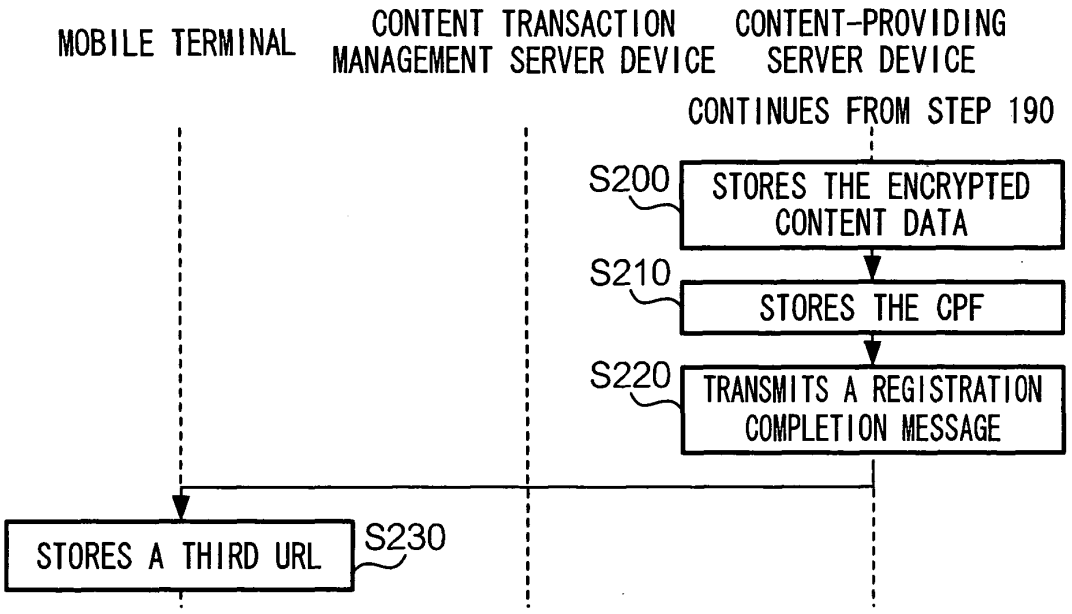

MOBILE TERMINAL
CONTENT TRANSACTION MANAGEMENT SERVER DEVICE
CONTENT-PROVIDING SERVER DEVICE
CONTINUES FROM STEP 190
S200
STORES THE ENCRYPTED CONTENT DATA
S210
STORES THE CPF
S220
TRANSMITS A REGISTRATION COMPLETION MESSAGE
STORES A THIRD URL
S230

FIG. 8

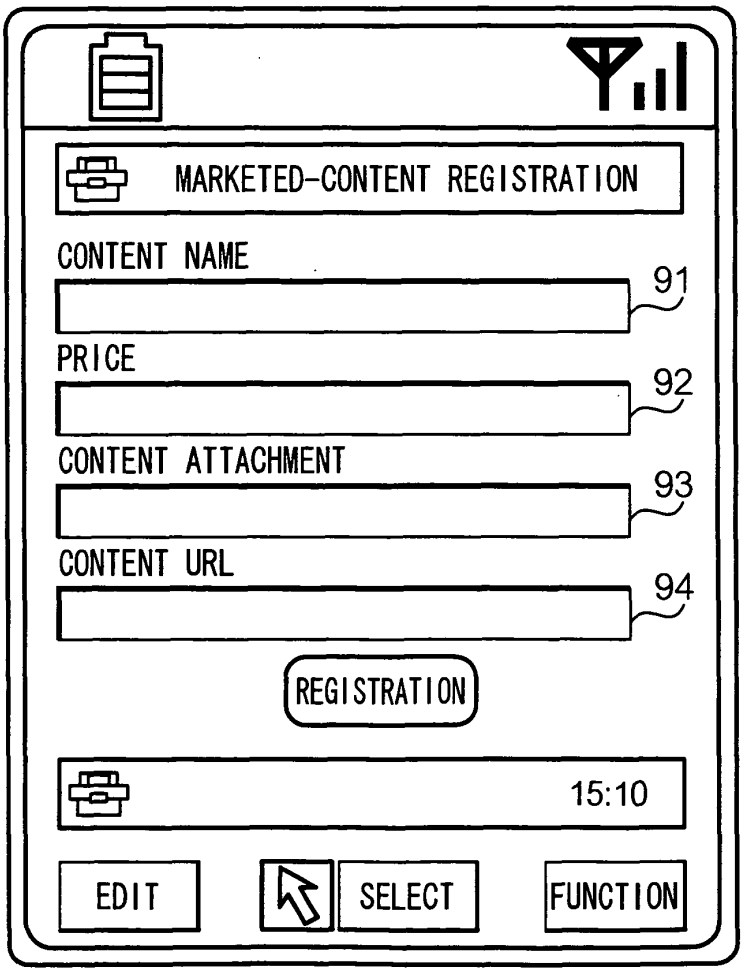

MARKETED-CONTENT REGISTRATION
CONTENT NAME
91
PRICE
92
CONTENT ATTACHMENT
93
CONTENT URL
94
REGISTRATION
15:10
EDIT
SELECT
FUNCTION

FIG. 9

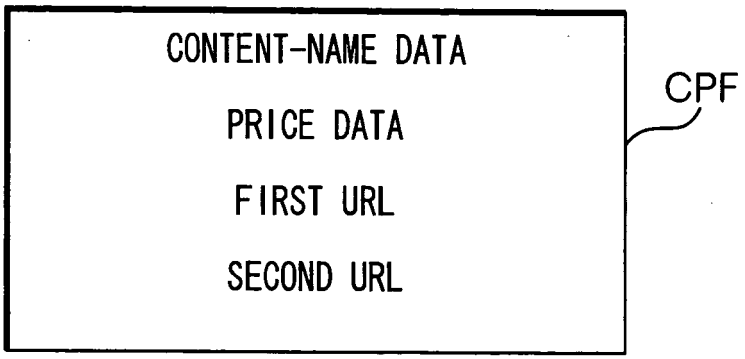

CONTENT-NAME DATA
PRICE DATA
FIRST URL
SECOND URL
CPF

FIG. 12

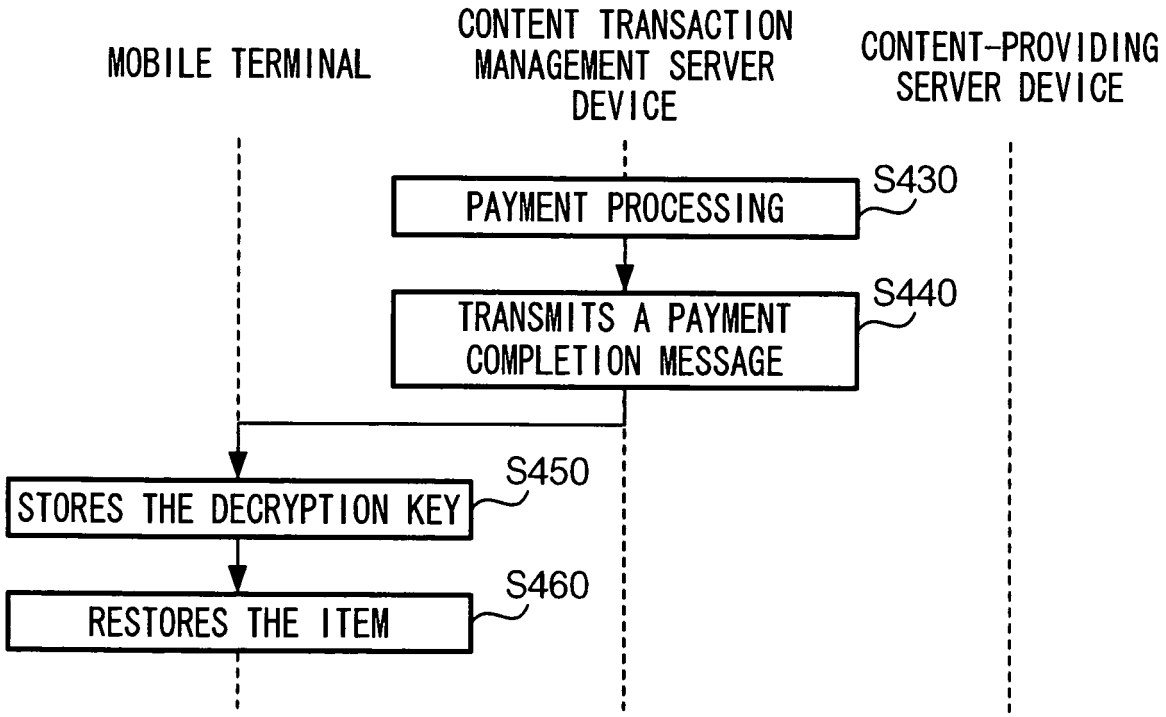

MOBILE TERMINAL
CONTENT TRANSACTION MANAGEMENT SERVER DEVICE
CONTENT-PROVIDING SERVER DEVICE
PAYMENT PROCESSING
S430
TRANSMITS A PAYMENT COMPLETION MESSAGE
S440
STORES THE DECRYPTION KEY
S450
RESTORES THE ITEM
S460

FIG. 10

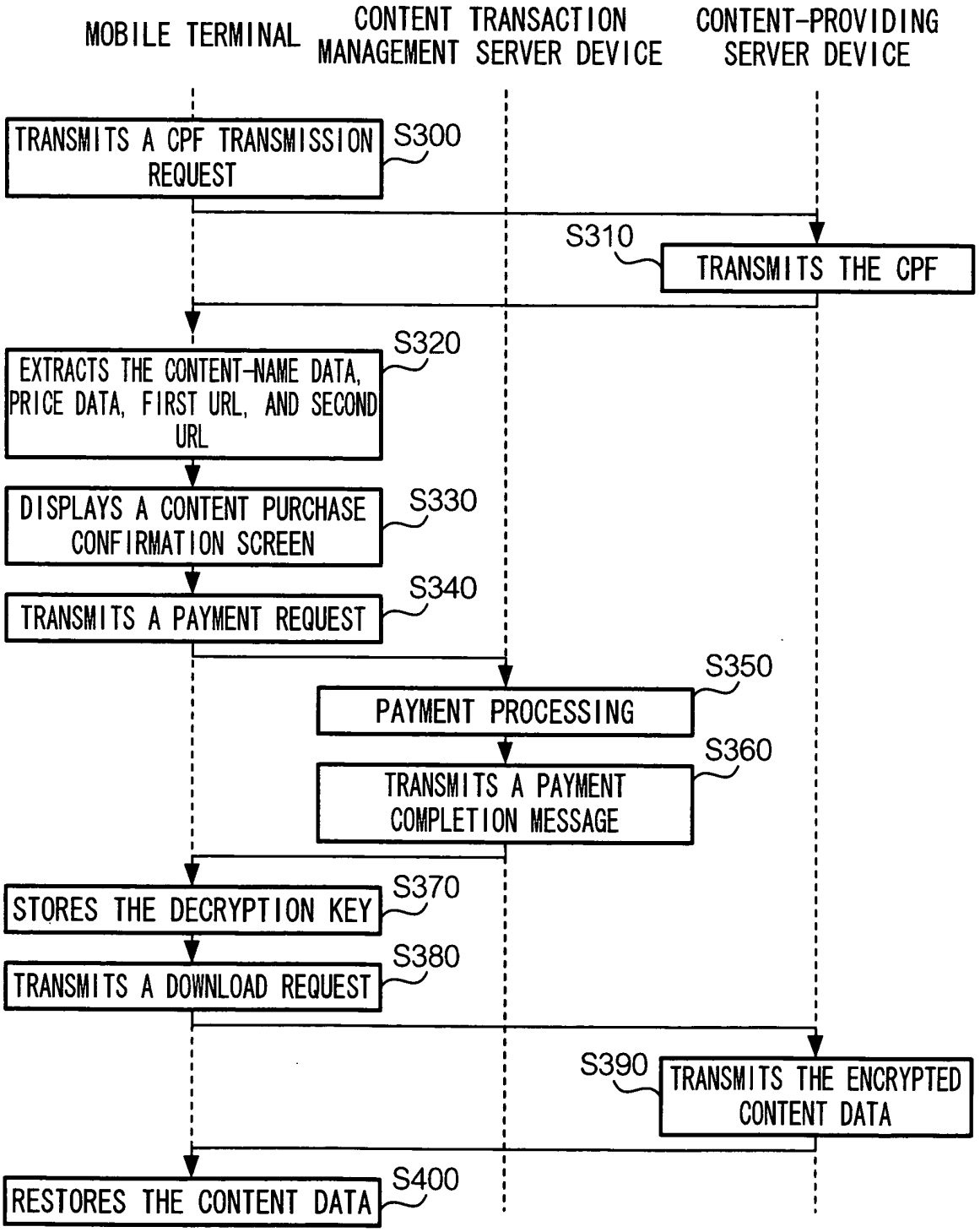
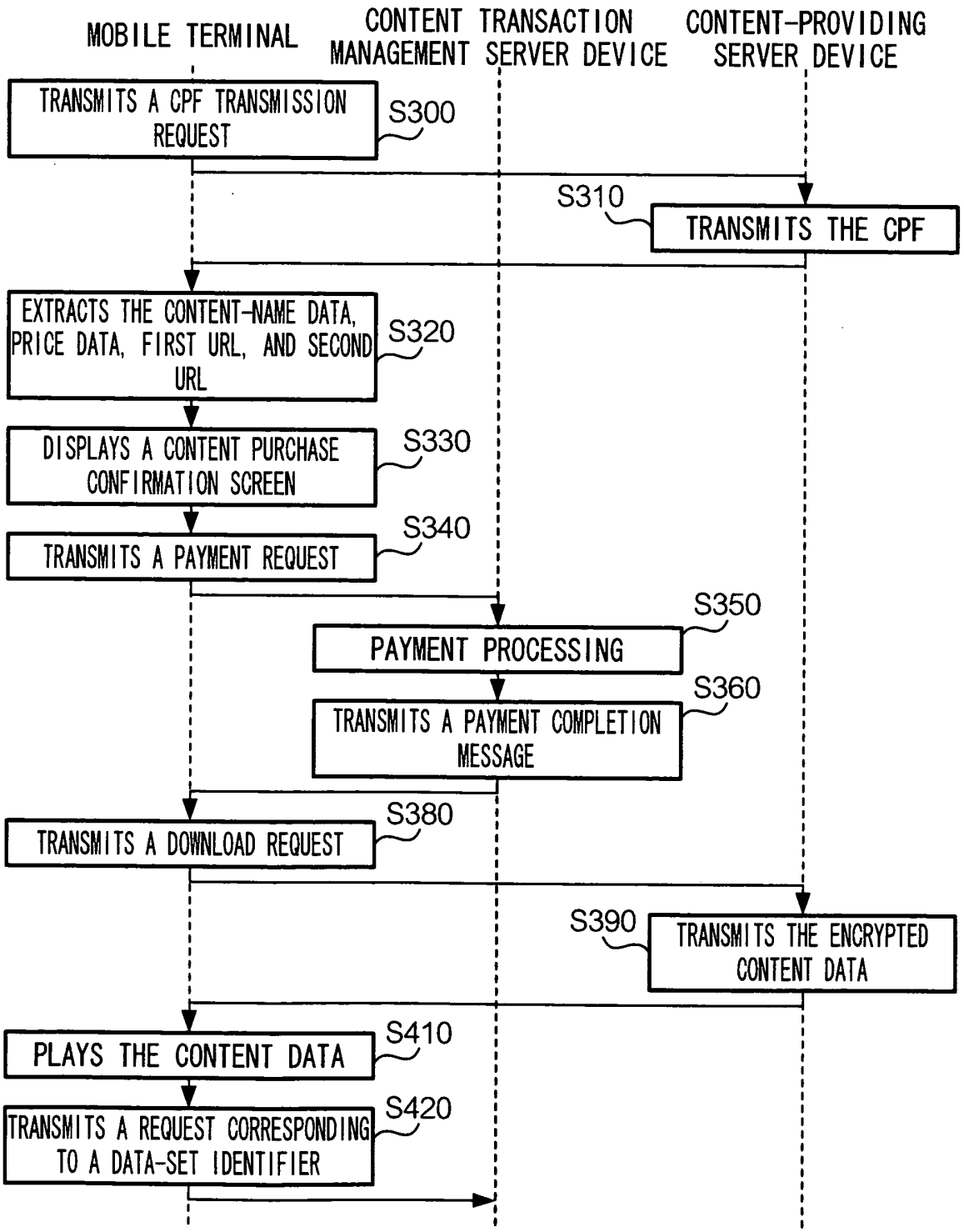

MOBILE TERMINAL
CONTENT TRANSACTION MANAGEMENT SERVER DEVICE
CONTENT-PROVIDING SERVER DEVICE
TRANSMITS A CPF TRANSMISSION REQUEST
S300
S310
TRANSMITS THE CPF
EXTRACTS THE CONTENT-NAME DATA, PRICE DATA, FIRST URL, AND SECOND URL
S320
DISPLAYS A CONTENT PURCHASE CONFIRMATION SCREEN
S330
TRANSMITS A PAYMENT REQUEST
S340
PAYMENT PROCESSING
S350
TRANSMITS A PAYMENT COMPLETION MESSAGE
S360
STORES THE DECRYPTION KEY
S370
TRANSMITS A DOWNLOAD REQUEST
S380
S390
TRANSMITS THE ENCRYPTED CONTENT DATA
RESTORES THE CONTENT DATA
S400

FIG. 11


MOBILE TERMINAL
CONTENT TRANSACTION MANAGEMENT SERVER DEVICE
CONTENT-PROVIDING SERVER DEVICE
TRANSMITS A CPF TRANSMISSION REQUEST
S300
S310
TRANSMITS THE CPF
EXTRACTS THE CONTENT-NAME DATA, PRICE DATA, FIRST URL, AND SECOND URL
S320
DISPLAYS A CONTENT PURCHASE CONFIRMATION SCREEN
S330
TRANSMITS A PAYMENT REQUEST
S340
S350
PAYMENT PROCESSING
S360
TRANSMITS A PAYMENT COMPLETION MESSAGE
S380
TRANSMITS A DOWNLOAD REQUEST
S390
TRANSMITS THE ENCRYPTED CONTENT DATA
S410
PLAYS THE CONTENT DATA
S420
TRANSMITS A REQUEST CORRESPONDING TO A DATA-SET IDENTIFIER

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/052009

A. CLASSIFICATION OF SUBJECT MATTER
G06Q20/00(2006.01)i, *G06F21/24*(2006.01)i, *G06Q10/00*(2006.01)i, *G06Q30/00*(2006.01)i, *H04L9/08*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q20/00, G06F21/24, G06Q10/00, G06Q30/00, H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2008
Kokai Jitsuyo Shinan Koho	1971-2008	Toroku Jitsuyo Shinan Koho	1994-2008

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 9-114787 A (Nippon Telegraph And Telephone Corp.), 02 May, 1997 (02.05.97), Par. Nos. [0012] to [0025]; Figs. 1 to 2 (Family: none)	1-2,5-7 3-4
Y	JP 2001-103047 A (PFU Ltd.), 13 April, 2001 (13.04.01), Par. Nos. [0023] to [0027]; Figs. 3 to 4 (Family: none)	3-4
Y	JP 2001-51960 A (Hitachi, Ltd.), 23 February, 2001 (23.02.01), Par. Nos. [0022] to [0024]; Fig. 1 (Family: none)	3-4

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 February, 2008 (26.02.08)	11 March, 2008 (11.03.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2007)

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- JP 2004013743 A **[0002]**